Part No. 210676-P
June 2002

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Business Policy Switch 2000

Software Version 2.0.5

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. June 2002.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

BayStack, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, and Optivity Policy Services are trademarks of Nortel Networks.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Introduction

These release notes for the Nortel Networks* Business Policy Switch 2000* software version 2.0.5 provide information about software and operational issues not included in the Business Policy Switch 2000 (BPS 2000) software version 2.0 guides.

To obtain the software version 2.0.5, download the following files from the Customer Support World Wide Web site:

- bps2k205_16.img (software file)
- bps2kdiag_2053.bin (diagnostics file)

You must download the diagnostics file as well as the software file.

Note: When you are downloading with a mixed (or Hybrid) stack, ensure that a BPS 2000 switch is Unit 1 and is the base unit. Ensure that you do not interrupt the download process; do not detach either the power cord or any of the network connections during download.

To obtain the Java* Device Manager (DM) software to manage the BPS 2000, download the following file from the Customer Support World Wide Web site:

- DM 5.5.3—You must upgrade the JRE software, which is on the web site, to version 1.3.0 at this time also.

Note: Ensure that you have upgraded to the BPS 2000 software v2.0 or later version when you use the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA. You must upgrade to the BPS 2000 software v2.0 or later version whether you are using a standalone BPS 2000, a stack of pure BPS 2000, or a mixed stack.

Note: When you create a policy that references shaping parameters, the 802.1p and Drop Precedence values must be changed either by using the system defaults or explicitly by the action.

These release notes provide information on version 2.0.5 and cover the following topics:

- "Stack Operational Mode after reset," next
- "Upgrading software" on page 5
- "Compatibility with BayStack 450 switches" on page 8
- "Documentation correction" on page 9
- "New features and enhancements" on page 10
- "Unknown multicast frame handling enhancement" on page 12
- "New Device Manager features" on page 12
- "Enhanced Web-based management features" on page 18
- "Enhancements to the console interface" on page 19
- "New and enhanced NNCLI commands for version 2.0.5" on page 20
- "Resolved issues" on page 33
- "Known issues" on page 36
- "Known limitations" on page 39
- "Related publications" on page 41
- "How to get help" on page 42

Stack Operational Mode after reset

When you reset the BPS 2000 switch to factory default settings, the Stack Operational Mode will not be reset. You must be especially aware of this when moving the switch between different stacks. For example, if you are working with a stack in Hybrid mode and you move that switch to a Pure BPS 2000 stack or a standalone configuration, you will have to manually set the Stack Operational Mode, even if you reset the switch to factory defaults.

The original documentation erroneously states that the Stack Operational Mode resets to a default value when you reset the switch to factory defaults.

Upgrading software

Note: Use the Command Line Interface (CLI), console interface (CI) menus, or the Web-based management system to upgrade to software version 2.0.5. For detailed instructions, refer to *Using the Business Policy Switch 2000 Version 2.0*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.0,* and *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.0.*

You use one of the management systems to upgrade or downgrade software. You follow a different procedure depending on whether you are using a Pure BPS 2000 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - — All BPS 2000 units must be running the same software version.
  - — All BayStack 410 units must be running the same software version.
  - — All BayStack 450 units must be running the same software version.
  - — All software versions must have the identical ISVN.

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack," next
- "Upgrading software in a Hybrid stack" on page 6

Upgrading software in a Pure BPS 2000 stack

To download, or upgrade, software in a Pure BPS 2000 stack:

1. Download the operational software, or agent, image.
2. Download the diagnostics image.

However, if you are currently using software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to version 2.0.5.

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software in a Hybrid stack

The physical order of the units and the unit numbering in the Hybrid stack does not affect the upgrading process at all. In addition, the cabling order regarding upstream/downstream neighbors does not affect the process.

Before you attempt to download new software (or upgrade software) to a Hybrid (mixed) stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate. The ISVNs and the accompanying software release are:

- ISVN 1
  - BayStack 410 or Bay Stack 450—version 3.1
  - BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
  - BayStack 410 or BayStack 450—versions 4.0, 4.1 and 4.2.
  - BPS 2000—versions 1.1, 1.1.1, 1.2, 2.0, and 2.0.5

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 7

Upgrading software when ISVN is 2

To upgrade a Hybrid stack to BPS 2000 software version 2.0.5 when the ISVN numbers of the units are 2:

1 Download the BPS 2000 image file.

The system resets.

2 Download the BPS 2000 diags file.

The system resets.

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software when ISVN is 1

To upgrade a Hybrid stack to BPS 2000 software version 2.0.5 when the ISVN numbers of the units are 1:

1 Download the BPS 2000 image file and the BayStack 450/410 file *simultaneously.*

Note: If you do not download both the BPS 2000 and BayStack 410/450 images simultaneously, the stack may not form.

The system resets.

2 Download the other BayStack 450 image file.

The system resets.

3 Download the BPS 2000 diags file.

The system resets.

4 Validate that the ISVN on both the BPS 2000 and the BayStack are 2.

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Compatibility with BayStack 450 switches

The BPS 2000 software version 2.0.5 is compatible with BayStack* 450 software versions 4.0, 4.1 and 4.2.

You can stack the BPS 2000 up to 8 units high. There are two types of stacks:

- Pure BPS 2000 —This stack has *only* BPS 2000 switches. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure BPS 2000 Mode.
- Hybrid—This stack has a combination of BPS 2000 switches *and* BayStack 450 and/or BayStack 410 switches. It is sometimes referred to as a mixed stack. The stack operational mode for this type of stack is Hybrid Stack.

All BPS 2000 switches in the stack must be running the identical version of software, and all the BayStack switches must be running the identical version of software.

When you are working with a mixed stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate. The ISVNs and the accompanying software release are:

- ISVN 1
  - — BayStack 410 or Bay Stack 450—version 3.1
  - — BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
  - — BayStack 10 or BayStack 450—versions 4.0, 4.1 and 4.2
  - — BPS 2000—versions 1.1, 1.1.1, 1.2, 2.0, and 2.0.5

In sum, the stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - — All BPS 2000 units must be running the same software version.
  - — All BayStack 410 units must be running the same software version.
  - — All BayStack 450 units must be running the same software version.
  - — All software versions must have the identical ISVN.

To find out which version of the BPS 2000 software is running, use the Console Interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the Console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

Refer to Appendix B of the *Using the Business Policy Switch 2000 Software Version 2.0* for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

Although the BPS 2000 software version 2.0.5 is compatible with BayStack 450 software versions 4.0 and 4.1, when you operate a mixed stack of BPS 2000 and BayStack 450 switches, some of the BayStack 450 software version 4.1 and 4.2 enhancements may not be accessible.

Documentation correction

Autonegotiation can be enabled on *every* supported fiber optic MDA except the BPS2000-2GE MDA. The previous documentation for BPS 2000 erroneously states that you cannot enable autonegotiation for *any* fiber optic port.

New features and enhancements

The following new features and enhancements are offered with the BPS 2000 software version 2.0.5:

- Support for Far End Fault Indication (FEFI)—When a fiber optic transmission link to a remote device fails, the remote device indicates the failure and the port is disabled. To use FEFI, you must enable autonegotiation on the port.

Note: FEFI will not work with the BPS 2000-2GE MDA because the BPS 2000-2GE MDA does not support autonegotiation.

- Increased support from 40 to 150 RMON alarms
- CLI support for RMON—See "New and enhanced NNCLI commands for version 2.0.5" on page 20 for a description of the new commands.
- SNMP support for downloading ASCII configuration files
- Settable Multicast MAC address for Spanning Tree Groups (STG)
  - Refer to "New and enhanced NNCLI commands for version 2.0.5" on page 20 for instructions on using this feature using the CLI.
  - Refer to "Enhanced Web-based management features" on page 18 for instructions on using this feature with Web-based management.
  - Refer to "Enhancements to the console interface" on page 19 for instructions on using this feature with the console interface.
- SNMP support for downloading diagnostics—See "New Device Manager features" on page 12.
- Device Manager enhancements—See "New Device Manager features" on page 12 for a description of the enhancements.
- Support for IGMP FAST LEAVE in Hybrid mode
- Unknown multicast frame handling enhancement
  - Refer to "Unknown multicast frame handling enhancement" on page 12 for explanation of this feature.
  - Refer to "New and enhanced NNCLI commands for version 2.0.5" on page 20 for instructions on using this feature using the CLI.
- BPS 2000-2GE MDA laser turned off when port disabled

- CLI enhancement for clearing Common Open Policy Services (COPS) server table—See "New and enhanced NNCLI commands for version 2.0.5" on page 20 for a description of the new command.
- Cannot enter broadcast address for MAC DA filtering
- CLI enhancement for saving configuration to NVRAM—See "New and enhanced NNCLI commands for version 2.0.5" on page 20 for a description of the new command.
- CLI enhancement for removing all VLANs—See "New and enhanced NNCLI commands for version 2.0.5" on page 20 for a description of the new command.
- BPS 2000 Image If Newer option added to the software download menu—If a newer image file is found, it will be downloaded and the switch will reset when the download process finishes successfully. Support for this feature has been added to the CLI, console, SNMP and Web-management.

The following new features and enhancements are offered with the BPS 2000 software version 2.0:

- Enhancement to BootP mode—Beginning with software version 2.0, the BootP or Last Address mode of BootP will always BootP for its IP configuration, regardless of whether a configured IP address is present, when the Stack BootP Mac Address Type is set to Base Unit Mac Address. If BootP is successful, the retrieved IP parameters are used by the switch or stack. The retrieved IP parameters are copied to the Last BootP IP parameters and overwrite any user-configured IP parameters. This feature applies only to a standalone BPS 2000 unit or to a stack consisting only of BPS 2000 units with the Stack Operational Mode set to Pure BPS 2000 Stack.
- Support for BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs
- QoS rate shaping
- No longer need to configure QoS meters if not metering traffic
- Improved QoS Wizard Web configuration pages
- QoS Quick Config Web configuration pages
- QoS filtering of multiple VLANs per Layer 2 filter
- Configurable VID for tagged STP BPDUs
- IP address for each switch in a stack
- MAC destination address (DA) filtering
- Port naming

- QoS policy enable or disable
- Enhanced Web QoS error reporting

Unknown multicast frame handling enhancement

By default, unknown multicast traffic is flooded to all ports in a VLAN. In situations where there is a multicast transmitter that is not doing IGMP and there are no multicast receivers, the traffic transmitted by the transmitter is flooded.

The new IGMP unknown mcast no flood CLI commands included in software version 2.0.5 allow you to send all unknown multicast traffic to IGMP static router ports only. This traffic will not be forwarded to dynamically discovered mrouter ports. If you want to forward unknown unicast traffic to certain ports only, you can set those ports as static mrouter ports.

- When disabled, BPS 2000 will treat unknown multicast traffic like broadcast traffic (flood). This is the default behavior.
- User setting for the unknown mcast no flood feature will be stored in NVRAM. In a stack, if settings on different units differ, Base Unit setting will take precedence. This feature can be enabled or disabled at any time.
- In a mixed BPS 2000/BayStack 450 stack, the unknown mcast no flood feature, if enabled, will take effect only on BPS 2000s. BayStack 450s will still flood unknown multicast traffic. Enabling this feature is not recommended in a mixed BPS 2000/BayStack 450 stack.
- It is suggested that this feature be used when IGMP snooping is enabled.

Refer to "IGMP CLI commands" on page 31 for a description of the new IGMP CLI commands for the unknown mcast no flood feature.

New Device Manager features

This section discusses the new Device Manager features included in software version 2.0.5 and covers the following topics:

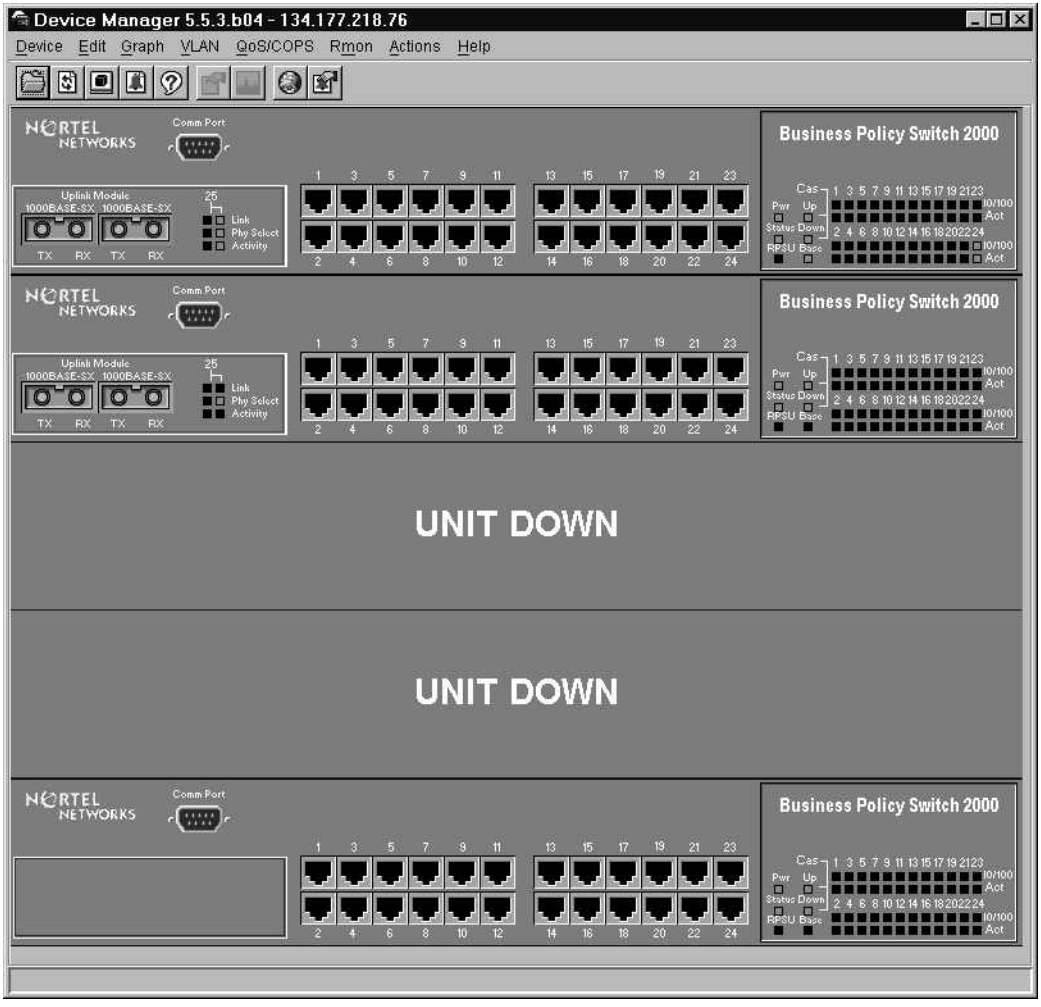
- "Device status within a stack," next
- "The management VLAN ID" on page 14

- "Base unit IP address" on page 15
- "IP addresses for the stack" on page 15
- "Designating the diagnostics file" on page 16
- "Downloading the ASCII config file" on page 16

Device status within a stack

The Device Manager will display devices that are down in a stack (Figure 1).

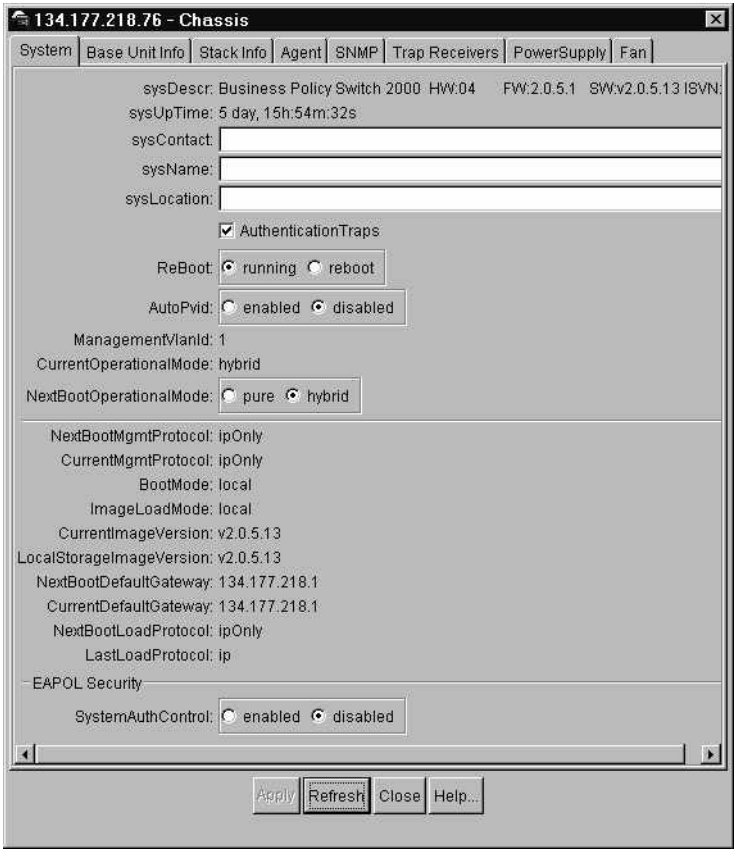
Figure 1 Device view



The management VLAN ID

You can now view the management VLAN ID in the System tab of the Edit Chassis dialog box (Figure 2).

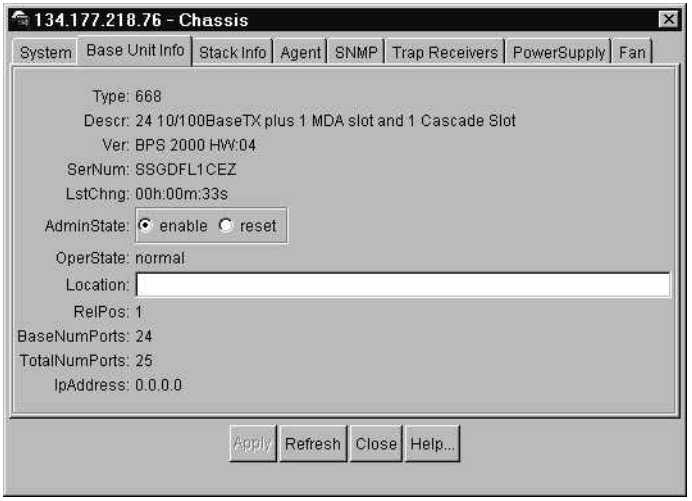
Figure 2 Edit Chassis dialog box—System tab



Base unit IP address

You can now view the Base Unit IP address in the Base Unit Info tab of the Edit Chassis dialog box (Figure 3).

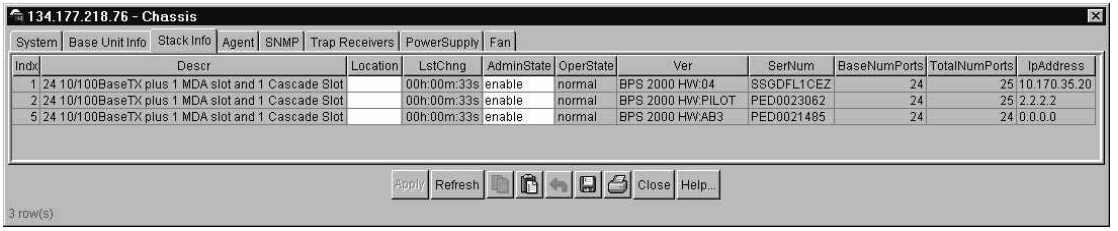
Figure 3 Edit Chassis dialog box—Base Unit Info tab



IP addresses for the stack

You can now view the IP addresses for the stack in the Stack Info tab of the Edit Chassis dialog box (Figure 4).

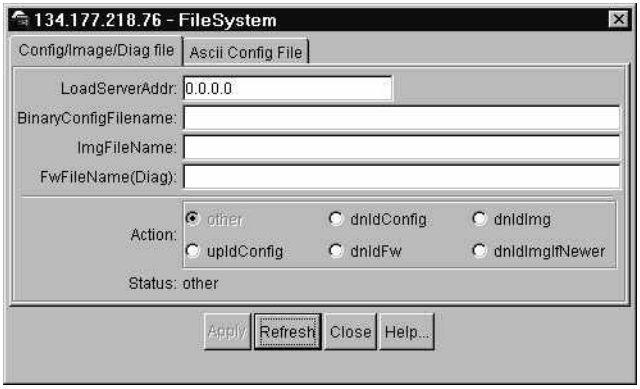
Figure 4 Edit Chassis dialog box—Stack Info tab



Designating the diagnostics file

You can now select the diagnostics file that is associated with the device in the Config/Image/Diag file tab of the Edit File System dialog box (Figure 5).

Figure 5 Edit File System dialog box—Config/Image/Diag file tab



Downloading the ASCII config file

To select the ASCII config file download options:

1 From the Device Manager menu bar, choose Edit > File System.

The File System dialog box opens with the Config/Image/Diag file tab displayed.

2 Click the Ascii Config File tab.

The Ascii Config File tab opens (Figure 6).

Figure 6 Edit File System dialog box—Ascii Config File tab

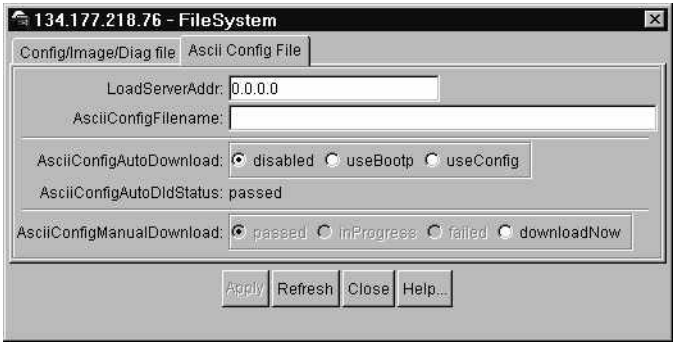


Table 1 describes the Ascii Config File tab fields.

Table 1 Ascii Config File tab fields

Field	Description
LoadServerAddr	Set the server address.
AsciiConfigFilename	Set the ASCII config filename.
AsciiConfigAutoDownload	The current ASCII config file download setting, which can be one of the following: • disabled • useBootp • useConfig If set to disabled, the device will not automatically download the ASCII config file.
AsciiConfigAutoDldStatus	Shows the status of the ASCII config file download.
AsciiConfigManualDownload	If downloadNow is selected, the ASCII config file will be downloaded immediately. Otherwise, download status is displayed.

Enhanced Web-based management features

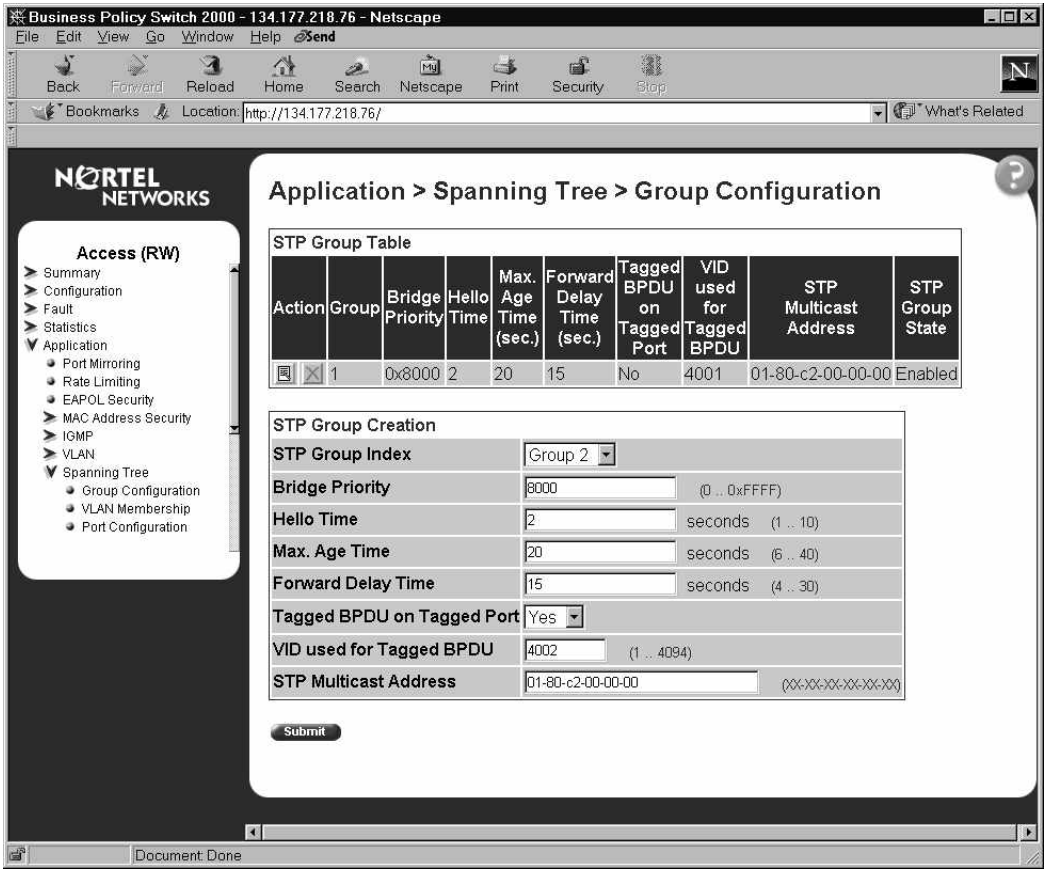
This section discusses the enhanced Web-based management features included in software version 2.0.5 and covers the following topics:

- "Setting the STG multicast MAC address," next

Setting the STG multicast MAC address

You can now set the STG multicast MAC address in the Application > Spanning Tree > Group Configuration window (Figure 7).

Figure 7 Group Configuration window


Business Policy Switch 2000 - 134.177.218.76 - Netscape
File Edit View Go Window Help Send
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://134.177.218.76/ What's Related
NORTEL NETWORKS
Application > Spanning Tree > Group Configuration
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Port Mirroring
Rate Limiting
EAPOL Security
MAC Address Security
IGMP
VLAN
Spanning Tree
Group Configuration
VLAN Membership
Port Configuration
STP Group Table
Action Group Bridge Priority Hello Time Max. Age Time (sec.) Forward Delay Time (sec.) Tagged BPDU on Tagged Port VID used for Tagged BPDU STP Multicast Address STP Group State
1 0x8000 2 20 15 No 4001 01-80-c2-00-00-00 Enabled
STP Group Creation
STP Group Index Group 2
Bridge Priority 8000 (0 .. 0xFFFF)
Hello Time 2 seconds (1 .. 10)
Max. Age Time 20 seconds (6 .. 40)
Forward Delay Time 15 seconds (4 .. 30)
Tagged BPDU on Tagged Port Yes
VID used for Tagged BPDU 4002 (1 .. 4094)
STP Multicast Address 01-80-c2-00-00-00 (XX-XX-XX-XX-XX-XX)
Submit
Document Done

Enhancements to the console interface

This section discusses the enhanced console interface features included in software version 2.0.5 and covers the following topic:

- "Setting the STG multicast MAC address," next

Setting the STG multicast MAC address

You can now set the STG multicast MAC address in the Main Menu > Spanning Tree Configuration > Spanning Tree Group Configuration menu (Figure 8).

Figure 8 Spanning Tree Group Configuration menu

```
Spanning Tree Group Configuration



              Create STP Group:             [ 1 ]
              Delete STP Group:             [   ]
              Bridge Priority:              [ 8000 ]
              Bridge Hello Time:            [ 2 seconds ]
              Bridge Max. Age Time:         [ 20 seconds ]
              Bridge Forward Delay Time:    [ 15 seconds ]
              Add    VLAN Membership:       [    1 ]
              Delete VLAN Membership:       [      ]
              Tagged BPDU on tagged port:   [ No  ]
              VID used for Tagged BPDU:     [ 4001 ]
              STP Multicast Address:        [ 01-80-c2-00-00-00 ]
              STP Group State:              [ Active   ]




Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

New and enhanced NNCLI commands for version 2.0.5

This section discusses the new and enhanced NNCLI commands included in software version 2.0.5 and covers the following topics:

- "Setting the STG multicast MAC address," next
- "Saving configuration to NVRAM" on page 21
- "Common Open Policy Services (COPS)" on page 22
- "Removing VLANs" on page 22
- "RMON CLI commands" on page 23
- "IGMP CLI commands" on page 31

Setting the STG multicast MAC address

The following command has been enhanced to allow setting of the STG multicast MAC address in software version 2.0.5:

spanning-tree

The `spanning-tree` command allows you to configure the spanning tree protocol. The syntax for the `spanning-tree` command is:

```
spanning-tree [stp <1-8>] [forward-time <4-30>] [hello-time
<1-10>] [max-age <6-40>] [priority <0-65535>] [tagged-bdpu
{enable|disable}] [tagged-bdpu-vid <1-4094>]
[multicast-address <H.H.H>]
```

The `spanning-tree` command is in the config command mode.

Table 2 describes the parameters and variables for the `spanning-tree` command.

Table 2 spanning-tree command parameters and variables

Parameters and variables	Description
stp <1-8>	Spanning tree group ID.
forward-time <4-30>	Set forward time.

Table 2 spanning-tree command parameters and variables (continued)

Parameters and variables	Description
hello-time <1-10>	Set hello time.
max-age <6-40>	Set maximum age.
priority <0-65535>	Set priority.
tagged-bdpu {enable|disable}	Enable/disable tagged BPDUs on tagged ports.
tagged-bdpu-vid <1-4094>	Set VLAN ID for tagged BPDUs
multicast-address <H.H.H>	Set spanning-tree multicast address.

Saving configuration to NVRAM

The following new command for saving configuration to NVRAM is offered with the BPS 2000 software version 2.0.5:

copy config nvram

The `copy config nvram` copies the current configuration to NVRAM. The syntax for the `copy config nvram` command is:

```
copy config nvram
```

The `copy config nvram` command is in the privExec command mode.

The `copy config nvram` command has no parameters or variables.

Note: The `copy config nvram` command is also periodically performed automatically

Common Open Policy Services (COPS)

The following command been enhanced in BPS 2000 software version 2.0.5 to allow the entire COPS server table to be cleared:

no cops server

The `no cops server` command removes COPS server configuration. When the variable is omitted, the entire COPS server table is cleared. The syntax for the `no cops server` command is:

```
no cops server [<A.B.C.D>]
```

The `no cops server` command is in the config command mode.

Table describes the parameters and variables for the `no cops server` command.

Table 3 no cops server command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to clear. Omitting this variable will clear the entire COPS server table.

Removing VLANs

The following command has been enhanced in BPS 2000 software version 2.0.5 to allow the removal of all VLANs:

no vlan

The `no vlan` command used with the variable omitted removes all VLANs. The syntax for the `no vlan` command is:

```
no vlan [<2-4094>]
```

Note: VLAN ID 1, the default management VLAN, cannot be deleted.

The `no vlan` command is in the config command mode.

Table 4 describes the parameters and variables for the `no vlan` command.

Table 4 no vlan command parameters and variables

Parameters and variables	Description
<2-4094>	ID of the VLAN to be removed. Omitting this variable will remove all VLANs except for VLAN 1, which cannot be deleted.

RMON CLI commands

This sections discusses the following new RMON CLI commands that are included in software version 2.0.5. and covers the following topics:

- "show rmon alarm," next
- "show rmon event" on page 24
- "show rmon history" on page 24
- "show rmon stats" on page 25
- "rmon alarm" on page 26
- "no rmon alarm" on page 27
- "rmon event" on page 28
- "no rmon event" on page 28
- "rmon history" on page 29
- "no rmon history" on page 30
- "rmon stats" on page 30
- "no rmon stats" on page 31

show rmon alarm

The `show rmon alarm` command displays information for RMON alarms. The syntax for the `show rmon alarm` command is:

```
show rmon alarm
```

The `show rmon alarm` command is in the privExec mode.

The `show rmon alarm` command has no parameters or variables. Figure 9 displays a sample output of the `show rmon alarm` command.

Figure 9 show rmon alarm command output

```
BPS2000#show rmon alarm
                                          Sample      Rising         Falling
Index Interval Variable                    Type  Threshold Event Threshold Event
----- -------- ------------------------- ------ --------- ----- --------- -----
1     30       ifInOctets.1              delta 500       1     10        1
```

show rmon event

The `show rmon event` command displays information regarding RMON events. The syntax for the `show rmon event` command is:

`show rmon event`

The `show rmon event` command is in the privExec mode.

The `show rmon event` command has no parameters or variables. Figure 10 displays a sample output of the `show rmon event` command.

Figure 10 show rmon event command output

```
BPS2000#show rmon event
Index Log Trap Description
----- --- ---- -----------------------------------------------------
1     Yes Yes  'Rising or Falling alarm on received octets'
```

show rmon history

The `show rmon history` command displays information regarding RMON history. The syntax for the `show rmon history` command is:

`show rmon history`

The `show rmon history` command is in the privExec mode.

The `show rmon history` command has no parameters or variables.

Figure 11 displays a sample output of the `show rmon history` command.

Figure 11 show rmon history command output

```
BPS2000#show rmon history
Index Unit/Port Buckets Requested Buckets Granted Interval
----- --------- ----------------- --------------- --------
1     1/1       15                15              30
2     1/2       15                15              30
3     1/3       15                15              30
4     1/4       15                15              30
5     1/5       15                15              30
6     1/6       15                15              30
7     1/7       15                15              30
8     1/8       15                15              30
9     1/9       15                15              30
10    1/10      15                15              30
11    1/11      15                15              30
12    1/12      15                15              30
13    1/13      15                15              30
14    1/14      15                15              30
15    1/15      15                15              30
16    1/16      15                15              30
17    1/17      15                15              30
18    1/18      15                15              30
19    1/19      15                15              30
20    1/20      15                15              30
--More--
```

show rmon stats

The `show rmon stats` command displays information regarding RMON statistics. The syntax for the `show rmon stats` command is:

```
show rmon stats
```

The `show rmon stats` command is in the privExec mode.

The `show rmon stats` command has no parameters or variables. Figure 12 displays a sample output of the `show rmon stats` command.

Figure 12 show rmon stats command output

```
BPS2000#show rmon stats
Index Unit/Port
----- ---------
1     1/1
2     1/2
3     1/3
4     1/4
5     1/5
6     1/6
7     1/7
8     1/8
9     1/9
10    1/10
11    1/11
12    1/12
13    1/13
14    1/14
15    1/15
16    1/16
17    1/17
18    1/18
19    1/19
20    1/20
--More--
```

rmon alarm

The `rmon alarm` command allows you to set RMON alarms and thresholds. The syntax for the `rmon alarm` command is:

```
rmon alarm <1-65535> <WORD> <1-2147483647> {absolute|delta}
rising threshold <-2147483648-2147483647> [<1-65535>]
falling-threshold <-2147483648-2147483647> [<1-65535>]
[owner <LINE>]
```

The `rmon alarm` command is in the config command mode.

Table 5 describes the parameters and variables for the `rmon alarm` command.

Table 5 rmon alarm command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the alarm entry.
<WORD>	The MIB object to be monitored. This is an OID, and for most available objects, an English name may be used.
<1-2147483647>	The sampling interval, in seconds.
absolute	Use absolute values (value of the MIB object is compared directly with thresholds).
delta	Use delta values (change in the value of the MIB object between samples is compared with thresholds).
rising-threshold <-2147483648-2147483647> [<1-65535>]	The first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event will be triggered.
falling-threshold <-2147483648-2147483647> [<1-65535>]	The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event will be triggered.
[owner <LINE>]	Specify an owner string to identify the alarm entry.

no rmon alarm

The `no rmon alarm` command turns off the RMON alarms. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon alarm` command is:

```
no rmon alarm [<1-65535>]
```

The `no rmon alarm` command is in the config command mode.

Table 6 describes the parameters and variables for the `no rmon alarm` command.

Table 6 no rmon alarm command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the alarm entry.

rmon event

The `rmon event` allows you to configure RMON event log and trap settings. The syntax for the `rmon event` command is:

```
rmon event <1-65535> [log] [trap] [description <LINE>]
[owner <LINE>]
```

The `rmon event` command is in the config command mode.

Table 7 describes the parameters and variables for the `rmon event` command.

Table 7 rmon event command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the event entry.
[log]	Record events in the log table.
[trap]	Generate SNMP trap messages for events.
[description *<LINE>*]	Specify a textual description for the event.
[owner *<LINE>*]	Specify an owner string to identify the event entry

no rmon event

The `no rmon event` turns off RMON event log and trap settings. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon event` command is:

```
no rmon event [<1-65535>]
```

The `no mon event` command is in the config command mode.

Table 8 describes the parameters and variables for the `no rmon event` command.

Table 8 no rmon event command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the event entry.

rmon history

The `rmon history` allows you to configure RMON history settings. The syntax for the `rmon history` command is:

`rmon history` *<1-65535> <LINE> <1-65535> <1-3600>* `[owner` *<LINE>*`]`

The `rmon history` command is in the config command mode.

Table 9 describes the parameters and variables for the `rmon history` command.

Table 9 rmon history command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the history entry.
<LINE>	Specify the port number to be monitored.
<1-65535>	The number of history buckets (records) to keep.
<1-3600>	The sampling rate (how often a history sample is collected).
[owner <LINE>]	Specify an owner string to identify the history entry.

no rmon history

The `no rmon history` turns off RMON history. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon history` command is:

`no rmon history [<1-65535>]`

The `no rmon history` command is in the config command mode.

Table 10 describes the parameters and variables for the `no rmon history` command.

Table 10 no rmon history command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the history entry.

rmon stats

The `rmon stats` command allows you to configure RMON statistics settings. The syntax for the `rmon stats` command is:

`rmon stats <1-65535> <LINE> [owner <LINE>]`

The `rmon stats` command is in the config command mode.

Table 11 describes the parameters and variables for the `rmon stats` command.

Table 11 rmon stats command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the stats entry.
[owner *<LINE>*]	Specify an owner string to identify the stats entry.

no rmon stats

The no `rmon stats` turns off RMON statistics. When the variable is omitted, all entries in the table are cleared. The syntax for the `no rmon stats` command is:

```
no rmon stats [<1-65535>]
```

The `no rmon stats` command is in the config command mode.

Table 12 describes the parameters and variables for the `no rmon stats` command.

Table 12 no rmon stats command parameters and variables

Parameters and variables	Description
<1-65535>	Unique index for the stats entry.

IGMP CLI commands

This sections discusses the following new IGMP CLI commands that are included in software version 2.0.5. and covers the following topics:

- "vlan igmp unknown-mcast-no-flood," next
- "show vlan igmp" on page 32
- "default vlan igmp unknown-mcast-no-flood" on page 33

vlan igmp unknown-mcast-no-flood

The `vlan igmp unknown-mcast-no-flood` command allows the user to block flooding of packets with unknown multicast address. Instead, the unknown multicast traffic will be sent only to IGMP static router ports. The syntax for the `vlan igmp unknown-mcast-no-flood` command is:

```
vlan igmp unknown-mcast-no-flood
```

The `vlan igmp unknown-mcast-no-flood` command is in the config command mode.

Table 13 describes the parameters and variables for the `vlan igmp unknown-mcast-no-flood` command.

Table 13 vlan igmp unknown-mcast-no-flood command parameters and variables

Parameters and variables	Description
enable	Enables flooding of packets with unknown multicast addresses. **Note:** The default parameter is enabled.
disable	Disables flooding of packets with unknown multicast addresses.

show vlan igmp

The `show vlan igmp` command displays whether flooding of packets with unknown multicast addresses is enabled or disabled. The syntax for the `show vlan igmp` command is:

`show vlan igmp {unknown-mcast-no-flood|<1-4094>}`

The `show vlan igmp` command is in the privExec command mode.

Table 14 describes the parameters and variables for the `show vlan igmp` command.

Table 14 show vlan igmp command parameters and variables

Parameters and variables	Description
unknown-mcast-no-flood	Displays whether flooding of packets with unknown multicast addresses is enabled or disabled.
<1-4094>	Displays IGMP setting for specified VLAN ID.

Figure 13 displays a sample output of the `show vlan igmp` command.

Figure 13 show vlan igmp command output

```
BPS2000#show vlan igmp unknown-mcast-no-flood
Unknown Multicast No-Flood:  Disabled
```

default vlan igmp unknown-mcast-no-flood

The `default vlan igmp unknown-mcast-no-flood` command enables flooding of packets with unknown multicast address. The syntax for the `default vlan igmp unknown-mcast-no-flood` command is:

```
default vlan igmp unknown-mcast-no-flood
```

The `default vlan igmp unknown-mcast-no-flood` command is in the privExec command mode.

The `default vlan igmp unknown-mcast-no-flood` command has no parameters or variables.

Resolved issues

The following issues were resolved in version 2.0.5:

- When configuring Port Mirroring on a specified MAC address, resetting the switch no longer causes instabilities in the system. (CR Q00155176)
- When deleting a VLAN member of a Spanning Tree Group (STG), the first port of the MLT is now correctly removed from the STG. (CR Q00316370)
- You no longer need to reboot the BPS 2000 switch when you add a policy where you configure shaping parameters. (CR Q00139108)
- When using Web management on a stack of BPS 2000 switches and accessing the Port Error Summary page, if the page contains more than six entries, the system will no longer hang. (CR Q00170933)
- The command `dot1dStpPortEnable.x` now works properly to disable a port. (CR Q00391212)
- The Redundant Power Supply Unit (RPSU) LED no longer returns the wrong value when using Device Manager. (CR Q00279588)

- You can now log in via the Web interface using RADIUS authentication. (CR Q00416483)
- You can now use the CLI to configure flow control for BPS 2000-2GE ports. (CR Q00415228)
- When autonegotiation is enabled for a Gigabit link, the flow control menu in the Web interface no longer offers the choice of Symmetric or Asymmetric. Flow control is disabled. (CR Q00416485)
- Sixteen character usernames cause RADIUS authentication to fail. Web and console interface now correctly limit usernames to 15 characters for RADIUS authentication. (CR Q00359668)
- The `show port-statistics` command has been added to all command modes. It was previously available only in the interface configuration mode. (CR Q00310716)
- In a Hybrid stack, when a station is moved to a different VLAN, it will properly communicate with the new VLAN (CR Q00384459)
- STP will now be correctly disabled on the monitor port when port mirroring is enabled. (CR Q00415229)
- If the connection is interrupted during the download of the diagnostics code, the switch will not try to use the incomplete diagnostics. (CR Q00417287)
- Timing issues during switch resets have been corrected so that large BPS 2000 stacks will no longer go into a loop when switches are reset. (CR Q00251306)
- The default global filter only applies to Ethernet II encapsulated packets. Default and customer-configured global filters can no longer corrupt IEEE 802.3 or SNAP (Subnetwork Access Protocol) encapsulated packets by modifying the Differentiated Services Code Point (DSCP) of the packets. (CR Q00230928)

Note: You cannot modify the DSCP of IEEE 802.3 or SNAP encapsulated packets.

The following issues were resolved in version 2.0.2.3:

- The allowable ranges for QoS Meter Committed Rate, Max Burst Rate, and Max Burst Duration in the CLI now correctly match the Web-based management ranges. (CR Q00209291)

- Malformed SNMP message packets are now discarded. These packets can no longer cause the SNMP task to crash, disabling SNMP, CLI and Web access. The BPS 2000 will no longer be affected by SNMP vulnerability issues documented on February 12, 2002 by CERT/CC in their SNMP advisory (VU#107186 and VU#854306).

The following issues were resolved in version 2.0:

- The `show log` and `clear log` CLI commands now function correctly. (CR Q00047028)
- The Web-based management system now correctly displays all configured VLANs. (CR Q00101635)
- IGMP Proxy now works correctly on tagged ports with multiple VLANs in multiple spanning tree groups. (CR Q00084861)
- It no longer takes a long time for the ASCII config file with extensive configurations to complete. (CR Q00091334)
- The flash synchronization was every 60 seconds. This synchronization now occurs very 2 minutes and 30 seconds.
- The setting of Learn by Ports in the MAC address-based security no longer changes to disabled after you reset the switch or stack. (CR Q00147573, Q00043550)
- You can now ping the switch if the MAC address-based learning security setting for the management port is set to Enabled. (CR Q0008448)
- The BPS 2000 switch no longer caches RADIUS responses (so that connections were authorized even when server is down). (CR Q00043170)

The stack stability was greatly enhanced in version 1.1.1.

The following issues were resolved in version 1.1:

- You can download BayStack 410 and BayStack 450 software images (and diagnostics) using the Device Manager in a mixed stack environment with Business Policy Switches.

  Using DM with a mixed stack and you choose Edit > File System, you can specify either the image for the BPS 2000 or the image for the BayStack, or both to download the software image(s).

- The BootP timeout for the BPS is now set to five minutes, which matches the BootP timeout value for the BayStack 450 switch. (CR 13161-1)

- BootP values set to either Always or When Needed are retained during a switch reset. (CR 126842-1)

The following issue was resolved in version 1.0.1:

- The ports on the BPS2000-4 TX MDA now autonegotiate correctly to 100 Mb/s full-duplex when they are connected to another BPS2000 port configured to autonegotiate.

Known issues

The following paragraphs discuss the known issues with the BPS 2000.

The following issues are known to exist in version 2.0.5 of the BPS 2000 software:

- When upgrading to 2.0.5 from 1.x, telnet access will be enabled, even if it was disabled before the upgrade. You must disable telnet access again, after the upgrade. (CR Q00391178)
- When you set a large number of RMON alarms, setting a short sampling interval for each alarm will cause the switch appear to be locked up as all CPU resources will be used to attempt the samples.(CR Q00411371)

  The workaround is to set larger sampling intervals for RMON alarms.
- The QoS shaping feature does not work in a stacked configuration; it works only in a BPS 2000 standalone unit. (CR Q00153202)
- QoS shaping is supported only on IP filters.
- The BPS 2000 Image If Newer option added to the software download menu does not work in a mixed stack. The download will fail with a message that the image is not newer.
- If STP is disabled for a switch, some DMLT ports may show incorrect Spanning Tree participation settings. (CR Q00425777)
- The CPU/Memory Utilization feature is unavailable in version 2.0.5 (CR Q00169353)

- When you are working with a mixed stack and download the v.2.0.x software for the BPS 2000 and the v.4.1.x software for the BayStack 450 *simultaneously*, the software may not load on all units.

  The workaround is to download the software separately to the BPS 2000 units and to the BayStack 450 units. The units reset after the software downloads in both cases.

- The flooded packets and filtered packets counters return incorrect results for the BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDA (they always display 0). (CR Q00137290)
- Nortel Networks recommends that you do not use MAC Address Security (BaySecure) on any MultiLink Trunk ports.
- When you renumber a stack of pure BPS 2000, check the port mirroring configuration. You may have to manually reconfigure the ports you want for port mirroring. (CR Q00156278)
- ASCII configuration file name maximum string length is 29, rather than 30, characters. (CRQ00107944)
- When you attempt to save the configuration to the TFTP server, it may not work the first time. (CR Q00153972)

  Workaround is to save it a second time, when it definitely saves.

- When you are using the CLI and attempt to set a 10/100 Mbps port to 1000 Mbps, the port mode resets to autonegotiation. (CR Q00153171)
- When you set the Authentication Trap and Autotopology to disabled and save the configuration file to the TFTP server, these two settings are not saved. (CR Q00153286)
- Before upgrading to BPS 2000 software version 1.2, save the software version 1.1 configuration as a binary configuration file in case you need to downgrade to software version 1.1.

Note: If you need to downgrade from BPS 2000 software version 1.2, save the configuration as a binary configuration file. The configuration files will be set to factory defaults as part of the downgrade process.

- If you are working with a mixed, or Hybrid, stack and are downgrading the software, the BPS 2000 units will reset to factory default but the BayStack 450 units will not default.

  The workaround is to default the entire stack.

- When you are working with QoS configurations and you delete a filter, that filter will continue to operate until you reset the BPS 2000. (CR Q00071760)
- When working in a mixed stack with BayStack 450 v.4.0/4.1 and BPS 2000, only the BPS 2000 displays the IP address of the stack. (CR Q00079143)
- When using the CLI and entering the IP address and mask in the form of A.B.C.D/<0-32>, you can also enter the values in the form of A.B.C.D/E.F.G.H.
- Occasionally when you have disabled MAC address-based security, the ports will still register as an intrusion. (CR Q00092007, Q00091998)

  The workaround is to reset the stack.

- The port speed and duplex you set using the ASCII configuration file may show incorrectly in the console display that shows port speed and duplex. The actual speed and duplex will be what you set with the configuration file, but the console display for these parameters may be incorrect. (CR Q00083014)

  The workaround is to use the CLI.

- When you are using DM to display the spanning tree group memberships, the port members may not display correctly. (CR Q00093350) Use the console interface (CI) menus, the CLI, or the Web-based management system to double-check the spanning tree group memberships.
- EAP configuration changes made at one console or using DM may not automatically display on other consoles. (CR Q00044484, CR Q00045315)

  The workaround is refresh the console and the correct data displays.

- If you rapidly add and delete VLANs (more than 1 per second) using DM, some of the VLANs may not be configured.

  The workaround is allow a few seconds to elapse between adding and deleting ports and VLANs if you are using DM.

- The ASCII configuration file does not support multiple spanning tree operations. (CR Q00088185)

  Use the CI menus, CLI, the Web-based management system, or DM to configure multiple spanning tree groups.

The following issues are known to exist in version 1.1 of the BPS 2000 software:

- The Multicast Group Membership table may display duplicate entries when the switch is in Distributed MultiLink Trunking (D-MLT) mode. However, the trunks function properly; this is a display problem only. (CR 138095-1)
- In a BPS 2000-only stack, the entire stack is reset to default values when you return the base unit to default values. (CR 145501-1)
- To disable a port that is part of a MultiLink Truck (MLT) group, use either Device Manager (DM) or the Console Interface (CI) management system menus (you can use the Telnet connection). With the Web-based management system, you may be unable to disable ports that are part of MLTs. (CR 146607-1)
- When the High Speed Flow Control Autonegotiation feature is set to enabled (the default), the port only advertises support for 1000 Mb/s operation, in full-duplex mode. If you experience problems between the Business Policy Switch and other network devices, set Autonegotiation to *disabled* on both sides of the link.
- Gigabit MDA
  - When viewing Active Phy information from the console interface, the console must be connected to the unit containing the Gigabit MDA (the BayStack 450-1SR MDA and the BayStack 450-1LLR MDA) to display the appropriate Phy information. Incorrect information may be displayed if you connect to a unit not containing a Gigabit MDA.
  - When you remove a Gigabit MDA from a switch, the Active Phy of the effected unit displays the new status. However, occasionally, the Active Phys of the other units in the stack or remote units will not display the new status.

Known limitations

The following limitations are known to exist:

- The current usable filters with software version 2.0.5 for the BPS are:
  - 200 policies
  - 100 interface groups
  - 200 IP filters and filter groups

— 24 IP filters with same Source Address (18 nested subnets)
— 14 Layer 2 filters and filter groups
— 200 meters
— 128 actions
— 62 shapers

Note: Each in-profile action, out-of-profile action, and statistics tracking session uses 1 filter each.

- Mixed stacks (hybrid stacks)—In order to upgrade BayStack 410 and BayStack 450 software in a hybrid stack, the stack must be fully redundant. All cables in the stack must be installed and operating properly. If the cables are not installed properly, the BayStack units will fail to upgrade. A message is displayed on consoles connected to BayStack 410 and BayStack 450 switches: `Primload Error - 2009 Switch will reset in 5 seconds...`
- You can configure protocol-based VLANs, with a sum total of "N" PID values not to exceed 14 (Table 15). If you are not running the spanning tree protocol, you have 15 PIDs available.

Table 15 Protocol and PID values

Protocol Name	Number of PID values (N)
Ip Ether2	2
Ipx 802.3	1
Ipx 802.2	1
Ipx Snap	2
Ipx Ether2Snap	2
AplTk Ether2Snap	2
Declat Ether2	1
DecOther Ether 2	10
Sna 802.2	2
Sna Ether2	1
NetBios 802.2	2
Xns Ether2	2
Vines Ether2	1

Table 15 Protocol and PID values (continued)

Protocol Name	Number of PID values (N)
Ipv6 Ether2	1
Usrdef	1
Rarp Ether2	1

For more information on Predefined Protocol Identifiers (PIDs), hexadecimal values, and associated protocols, refer to *Using the Business Policy Switch 2000 Software Version 2.0*.

Related publications

For more information about the BPS 2000 switch, refer to:

- *Using the Business Policy Switch 2000 Software Version 2.0* (part number 208700-C)
- *Using Web-Based Management for the Business Policy Switch 2000 Software Version 2.0* (part number 209570-C)
- *Reference for the Business Policy Switch 2000 Management Software Version 2.0* (part number 209322-C)
- *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.0* (part number 212160-B)
- *Getting Started with the Business Policy Switch 2000 Management Software* (part number 209321-A)
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A)
- *Installing Media Dependent Adapters (MDAs)* (part number 302403-H)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)
- *Installing Optivity Policy Services* (part number 306972-E Rev 00)
- *Managing Policy Information in Optivity Policy Services* (part number 306969-F Rev 00)
- *Release Notes for Optivity Policy Services Version 2.0* (part number 306975-E Rev 00)

- *Task Map - Installing Optivity Policy Services Product Family* (part number 306976-D Rev 00)
- *Known Anomalies for Optivity Policy Services Version 2.0* (part number 306974-E Rev 00)
- *Using the Optivity Quick2Config 2.2 Client Software* (part number 207810-B)
- *Installing and Administering Optivity Quick2Config 2.2* (part number 207890-B)
- *Configuring Business Policy Switches with Optivity Quick2Config 2.2* (part number 311208-A)
- *Release Notes for Optivity Quick2Config for Business Policy Switch 2000, v.2.2.1* (part number 310621-A)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat* Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.